CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10) Applicant(s): **Richard DOLLET**			Docket No. **09669/010001**
Serial No.	Filing Date **September 17, 2001**	Examiner	Group Art Unit 09/936685

Invention: **METHOD OF SECURE LOADING OF DATA BETWEEN SECURITY MODULES**

I hereby certify that the following correspondence:

PCT National Phase Application

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on

September 17, 2001
(Date)

Rhonda L. Parker
(Typed or Printed Name of Person Mailing Correspondence)

Rhonda L. Parker
(Signature of Person Mailing Correspondence)

EL656798874US
("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

EL656798874US

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 76.0543	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 00/ 00680	Date du dépôt international *(jour/mois/année)* 17/03/2000	(Date de priorité (la plus ancienne) *(jour/mois/année)* 17/03/1999
Déposant SCHLUMBERGER SYSTEMES et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé**,

   [X] le texte est approuvé tel qu'il a été remis par le déposant

   [ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

   [ ] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [X] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PC[illegible]R 00/00680

A. CLASSEMENT DE L'OBJET DE LA DEM[illegible]
CIB 7 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) abrégé colonne 3, ligne 52 -colonne 4, ligne 35 colonne 5, ligne 55 -colonne 7, ligne 40 colonne 8, ligne 5 - ligne 10 ---	1-3,6,8, 9
A	US 4 731 840 A (MNISZEWSKI SUSAN M ET AL) 15 mars 1988 (1988-03-15) abrégé colonne 2, ligne 34 -colonne 3, ligne 25 revendication 1 ---	1-9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) abrégé page 5, ligne 17 - ligne 30 page 7, ligne 20 -page 10, ligne 18 -----	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 mai 2000	06/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Gautier, L

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PC[redacted]R 00/00680

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5517567	A	14-05-1996	NONE	
US 4731840	A	15-03-1988	NONE	
FR 2681165	A	12-03-1993	NONE	

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 570041
FR 9903329

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	US 5 517 567 A (EPSTEIN PHILIP) 14 mai 1996 (1996-05-14) * abrégé * * colonne 3, ligne 52 - colonne 4, ligne 35 * * colonne 5, ligne 55 - colonne 7, ligne 40 * * colonne 8, ligne 5 - ligne 10 *	1-3,6,8, 9
A	US 4 731 840 A (MNISZEWSKI SUSAN M ET AL) 15 mars 1988 (1988-03-15) * abrégé * * colonne 2, ligne 34 - colonne 3, ligne 25 * * revendication 1 *	1-9
A	FR 2 681 165 A (GEMPLUS CARD INT) 12 mars 1993 (1993-03-12) * abrégé * * page 5, ligne 17 - ligne 30 * * page 7, ligne 20 - page 10, ligne 18 *	1-9

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)

H04L
G07F

1

Date d'achèvement de la recherche	Examinateur
10 janvier 2000	Gautier, L

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

Translation

3

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

9/936685

Applicant's or agent's file reference 76.0543	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/00680	International filing date (*day/month/year*) 17 March 2000 (17.03.00)	Priority date (*day/month/year*) 17 March 1999 (17.03.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant SCHLUMBERGER SYSTEMES		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
08 September 2000 (08.09.00)	02 July 2001 (02.07.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/00680

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-9, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the claims:

pages 1-9, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☒ the drawings:

pages 1/2-2/2, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 4-9

because:

☐ the said international application, or the said claims Nos. _____ relate to the following subject matter which does not require an international preliminary examination *(specify)*:

☒ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. 4-9 are so unclear that no meaningful opinion could be formed *(specify)*:

See separate sheet.

☐ the claims, or said claims Nos. _____ are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for said claims Nos. _____.

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Box III

See Box VIII, paragraph 1, concerning Claims 4-9.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-3	YES
	Claims		NO
Inventive step (IS)	Claims	1-3	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-3	YES
	Claims		NO

2. Citations and explanations

I

The following documents (D) have been considered in writing this preliminary examination report:

D1: US-A-5 517 567

D2: US-A-4 731 840

D3: FR-A-2 61 165.

II

The present application concerns a secure method for loading secret data from a first security module to at least a second security module. The invention is applicable to telephone systems, the first module being in a management server and the second module being in a public telephone; the second module ensures that a user card inserted into the public telephone is valid.

When the public telephone connects to the server, it is unavailable to all users. The connection therefore usually occurs at night in off-line mode.

In order to reduce the risk of fraud involving hacking into the communication network connecting the server to the public telephones and thereby obtaining secret data,

operators regularly have to modify the secret data of the second security module of a public telephone on the basis of the secret data stored in the first security module.
According to the invention, random data is used to load the secret data, which enables the loading security to be improved by perfectly diversifying the transmitted data. As a result of the data diversification, a fraudulent person hacking into the network and gathering transmitted data never obtains the same encryption value.
Moreover, the second module has a non-volatile memory and a volatile memory. The presence of two memories, one of which is non-volatile, enables exchanges to be carried out in off-line mode. Indeed, the said random data is not lost when the security module is switched off.
The novel way in which the data (secret and random) is exchanged between the volatile and non-volatile memories of the second module and between the second and first modules, with the advantages described above, cannot be derived from the cited documents and is therefore considered to involve an inventive step.

Consequently, Claims 1-3 satisfy the requirements of PCT Article 33(3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. If the applicant is aware of a document representing the prior art as described in the introductory part of the description on pages 1 and 2 ("... terminal management systems exist in which...", "... Although this method enables secret data to be loaded between first and second security modules..."), it should identify that document in accordance with PCT Rule 5.1(a)(ii).
In that case, in order to comply with PCT Rule 6.3(b), independent Claim 1 should be **correctly** presented in two-part form, with features known from that document being mentioned in the first part.

If no such document is known to the applicant, the applicant should mention and briefly summarise documents D1-D3 in the introductory part of the description. The preamble of the claims should then be amended so as to reflect the features known from the closest document (probably D1).
Finally, the part of the description in which the technical problems in question and the solution to those problems are presented must then be amended in the light of those documents (PCT Rule 5.1(a)(iii); and PCT Examination Guidelines, Chapter II-4.6).

2. In order to satisfy the requirements of PCT Rule 5.1(a)(iii), the introductory part of the description should be made consistent with the new claims submitted by the applicant.

3. Reference signs mentioned in the description ought to

VII. Certain defects in the international application

appear in the drawings, and vice versa (see PCT Rule 11.13(l)). On this issue, the description on page 4 concerning Figure 2 (lines 20-30) indicates that the second module SAM contains an algorithm ALGOP **as well as secret data DATA.** However, Figure 2 shows no data DATA in the module SAM. The description then reads: "...In order to modify secret data...". What secret data? The data DATA? Figure 2 likewise fails to elucidate this problem.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1a. Claims 4 and 5 are unclear (PCT Article 6) in that they refer to first and second commands (ASKLOADING and ADMINRECOVER) without indicating the origin of these commands and the means by which they are sent. Do they emanate from module S? From module SAM? From a higher management level? If the latter applies, this management level has not been mentioned previously in the claims. Furthermore, there is no previous indication in the claims of how modules S and SAM communicate with that management level and why.

The Examining Authority therefore suggests that these claims be deleted.

1b. Since they are dependent on the aforementioned Claims 4 and 5, Claims 6-9 lack clarity for the same reason.

2. Dependent Claim 2 is unclear in that it cannot be dependent on **one of** the preceding claims. Indeed, Claim 1 is its only preceding claim.

09/936685

T 4

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 76.0543 pct	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR00/00680	Date du dépot international *(jour/mois/année)* 17/03/2000	Date de priorité *(jour/mois/année)* 17/03/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/08		
Déposant SCHLUMBERGER SYSTEMES et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 8 feuilles, y compris la présente feuille de couverture.

   ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

I	☒	Base du rapport
II	☐	Priorité
III	☒	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☒	Irrégularités dans la demande internationale
VIII	☒	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
08/09/2000	02.07.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Dechmann, J-L N° de téléphone +49 89 2399 8826

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/00680

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-9 version initiale

Revendications, N°:

1-9 version initiale

Dessins, feuilles:

1/2-2/2 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

☐ de la description, pages :

☐ des revendications, n^{os} :

☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

III. Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

1. La question de savoir si l'objet de l'invention revendiquée semble être nouveau, impliquer une activité inventive (ne pas être évident) ou être susceptible d'application industrielle n'a pas été examinée pour ce qui concerne :

   ☐ l'ensemble de la demande internationale.

   ☒ les revendications n^{os} 4-9.

parce que :

   ☐ la demande internationale, ou les revendications n^{os} en question, se rapportent à l'objet suivant, à l'égard duquel l'administration chargée de l'examen préliminaire international n'est pas tenue effectuer un examen préliminaire international *(préciser)* :

   ☒ la description, les revendications ou les dessins (*en indiquer les éléments ci-dessous*), ou les revendications n^{os} 4-9 en question ne sont pas clairs, de sorte qu'il n'est pas possible de formuler une opinion valable *(préciser)* :
   voir feuille séparée

   ☐ les revendications, ou les revendications n^{os} en question, ne se fondent pas de façon adéquate sur la description, de sorte qu'il n'est pas possible de formuler une opinion valable.

   ☐ il n'a pas été établi de rapport de recherche internationale pour les revendications n^{os} en question.

2. Le listage des séquences de nucléotides ou d'acides aminés n'est pas conforme à la norme prévue dans l'annexe C des instructions administratives, de sorte qu'il n'est pas possible d'effectuer un examen préliminaire international significatif:

   ☐ le listage présenté par écrit n'a pas été fourni ou n'est pas conforme à la norme.

   ☐ le listage sous forme déchiffrable par ordinateur n'a pas été fourni ou n'est pas conforme à la norme.

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-3
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-3
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-3
	Non :	Revendications	

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

III. Non-Formulation d'opinion quant à la nouveauté, l'activité inventive et l'application industrielle

Voir la section VIII-1, concernant les revendications 4 à 9.

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

I

Les documents (D) suivants ont été pris en compte pour l'établissement du rapport d'examen préliminaire:

D1: US-A-5 517 567
D2: US-A-4 731 840
D3: FR-A-2 681 165

II

La présente demande concerne un procédé de chargement sécurisé de données secrètes à partir d'un premier module de sécurité vers au moins un deuxième module de sécurité. L'invention trouve son application dans la téléphonie, le premier module étant dans un serveur d'administration et le deuxième module dans un publiphone, le deuxième module garantissant la validité d'une carte utilisateur introduite dans le publiphone.
Lorsque le publiphone se connecte au serveur, il est indisponible à tout utilisateur. La connexion se fait donc généralement la nuit en mode off-line.
Afin de diminuer les risques de fraude consistant à espionner le réseau de communication reliant le serveur et les publiphones et ainsi de découvrir les données

secrètes, les opérateurs sont amenés à modifier régulièrement les données secrètes du deuxième module de sécurité d'un publiphone à partir des données secrètes contenues dans le premier module de sécurité.
Selon l'invention, une donnée aléatoire est utilisée pour le chargement des données secrètes permettant d'améliorer la sécurité du chargement en diversifiant parfaitement les données transmises. La diversification des données permet qu'un fraudeur qui espionne le réseau et récupère les données transmises n'obtient jamais une même valeur de chiffrement.
De plus le deuxième module comporte une mémoire non-volatile et une mémoire volatile. Le fait d'avoir deux mémoires dont une non-volatile, permet les échanges en mode off-line. En effet ladite donnée aléatoire n'est pas perdue lorsque le module de sécurité est mis hors tension.
La façon originale dont les données (secrètes et aléatoires) sont échangées entre la mémoire volatile et la mémoire non volatile du deuxième module et entre le deuxième module et le premier module, et ayant les avantages décrits ci-dessus, n'est pas dérivable des documents cités et une activité inventive est donc reconnue.

Les revendications 1-3 remplissent donc les exigences de l'Article 33(3) PCT.

VII. Irrégularités dans la demande internationale

1. Si le Demandeur a connaissance d'un document représentant l'état de la technique tel qu'il le décrit à l'introduction de la description pages 1 et 2 ("...il existe des systèmes d'administration de terminaux qui comportent...", "...Bien que ce procédé permette un chargement de données secrètes entre un premier et un deuxième modules de sécurité..."), il lui est demandé d'identifier ce document conformément à la Règle 5.1(a)(ii) du PCT.
   Dans ce cas, en vue de remplir les conditions de la Règle 6.3(b) PCT, la revendication indépendante 1 devra être **correctement** présentée en deux parties, les caractéristiques connues de ce document étant indiquées dans la première partie.

   Dans le cas contraire, le Demandeur est prié de mentionner et de brièvement

analyser les documents D1 à D3 dans la partie introductive de la description. Le préambule des revendications devra alors être modifié pour prendre en compte les caractéristiques connues du document le plus proche (vraisemblablement D1).
Enfin, la partie de la description exposant les problèmes techniques traités et la solution apportée à ces problèmes devra alors être révisée eu égard à ces documents (Règle 5.1(a)(iii) PCT et Directives PCT Chap. II-4.6).

2. En vue de remplir les conditions énoncées à la Règle 5.1(a)(iii) PCT, la partie introductive de la description devra être mise en conformité avec les nouvelles revendications proposées par le Demandeur.

3. Les signes de référence mentionnés dans la description devraient apparaître dans les dessins, et vice versa (Cf. Règle 11.13 (l) PCT). A cet égard, la description page 4 concernant la figure 2 (lignes 20-30) mentionne que le deuxième module SAM comporte un algorithme ALGOP **ainsi que des données secrètes DATA**. Cependant la Figure 2 ne montre aucune donnée DATA dans le modules SAM. Ensuite la description mentionne: "...Afin de modifier une donnée secrète...". Quelle donnée secrète? Les données DATA? La Figure 2 n'éclaircie pas non plus sur ce problème.

VIII. Observations relatives à la demande internationale

1a. Les revendications 4 et 5 ne sont pas claires (Article 6 PCT) en ce qu'elles mentionnent des première et deuxième commandes (ASKLOADING et ADMINRECOVER) sans préciser d'où viennent ces commandes et par quels moyens elles sont envoyées. Proviennent-elles du module S? du module SAM? d'une administration supérieure? Si c'était le 3ème cas, cette administration n'a jamais été introduite auparavant dans les revendications. De plus il n'a jamais été spécifié auparavant dans les revendications comment les modules S et SAM sont en communication avec cette administration et pourquoi.

Il est donc suggéré de supprimer ces revendications.

1b. Les revendications 6 à 9, lorsqu'elles sont dépendantes de ces revendications 4 et 5, manquent donc de clarté pour les mêmes raisons.

2. La revendication dépendante 2 n'est pas claire en ce qu'elle ne peut dépendre de l'une **des** revendications précédentes. En effet, la revendication 1 est la seule qui la précède.

PATENT
ATTORNEY DOCKET NO. 09669/010001

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: **METHOD OF SECURE LOADING OF DATA BETWEEN SECURITY MODULES**

APPLICANTS: **Richard DOLLET**

"EXPRESS MAIL" Mailing Label Number: EL656798874US
Date of Deposit: September 17, 2001